

Số: /VHTT-TT

Định Hóa, ngày tháng 5 năm 2024

V/v cảnh báo chiến dịch tấn công
sử dụng mã độc RAT để thực hiện
hành vi trái phép

Kính gửi:

- Các cơ quan, ban, ngành, đoàn thể huyện;
- Ủy ban nhân dân các xã, thị trấn;
- Các doanh nghiệp viễn thông trên địa bàn huyện.

Thực hiện Công văn số 1218/STTTT-CNTT ngày 27/5/2024 của Sở Thông tin và Truyền thông về cảnh báo chiến dịch tấn công sử dụng mã độc RAT để thực hiện hành vi trái phép.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, đơn vị, góp phần đảm bảo an toàn cho các hệ thống thông tin dùng chung. Phòng Văn hóa và Thông tin cảnh báo chiến dịch tấn công sử dụng mã độc RAT để thực hiện hành vi trái phép (*Chi tiết tại Phụ lục kèm theo*), đồng thời khuyến nghị đến các cơ quan, đơn vị UBND các xã, thị trấn, các doanh nghiệp viễn thông thực hiện một số nội dung như sau:

1. Kiểm tra, rà soát hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi mã độc trên. Chủ động theo dõi các thông tin liên quan đến mã độc từ hãng nhằm thực hiện nâng cấp lên phiên bản mới nhất để tránh nguy cơ bị tấn công.

2. Tăng cường giám sát và phối hợp với Phòng Văn hóa và Thông tin thực hiện phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi các thông tin liên quan đến chiến dịch tấn công mạng và kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

3. Tuyên truyền thường xuyên, liên tục bằng hình thức phù hợp tới toàn thể cán bộ, công chức, viên chức, người lao động của cơ quan, đơn vị nhằm nâng cao nhận thức và trang bị kỹ năng đảm bảo an toàn thông tin trên không gian mạng.

Trên đây là thông tin và khuyến nghị về chiến dịch tấn công sử dụng mã độc RAT để thực hiện hành vi trái phép và lỗ hổng an toàn thông tin trên Foxit PDF Reader gây ảnh hưởng đến các hệ thống thông tin, đề nghị các cơ quan, đơn vị UBND các xã, thị trấn, doanh nghiệp viễn thông thực hiện. Trong trường hợp

cần thiết có thể liên hệ đầu mối hỗ trợ của Phòng Văn hóa và Thông tin: Ông Ngô Nguyên Long, công chức biệt phái, số điện thoại 0943905333./.

Nơi nhận:

- Như trên;
- Lãnh đạo UBND huyện;
- Lưu: VT, VHTT.

**KT. TRƯỞNG PHÒNG
PHÓ TRƯỞNG PHÒNG**

Ngô Hoàng

PHỤ LỤC THÔNG TIN CHI TIẾT VỀ MÃ ĐỘC
(Kèm theo Công văn số: / VHTT-TT ngày / 5/2024
của Phòng Văn hóa và Thông tin)

1. Thông tin chi tiết về lỗ hổng an toàn thông tin trên Foxit PDF Reader

Gần đây, qua công tác giám sát an toàn không gian mạng đã phát hiện hành vi sử dụng file PDF nhằm khai thác lỗ hổng trên phần mềm Foxit Reader khiến người dùng thực thi các câu lệnh độc hại trên thiết bị của mình. Hiện lỗ hổng đang được khai thác bởi nhiều nhóm tấn công trong môi trường thực tế.

Qua quá trình phân tích, các chuyên gia bảo mật đã phát hiện nhiều chủng mã độc, công cụ độc hại được sử dụng trong chuỗi lây nhiễm như: VenomRAT, Agent-Tesla, Remcos, NjRAT, NanoCore RAT, Pony, Xworm, AsyncRAT và DCRat.

Lỗ hổng trên phần mềm Foxit PDF Reader đã bị khai thác bởi nhiều nhóm tấn công khác nhau với điểm chung là mã độc được phát tán dưới dạng các file PDF độc hại. Một số chiến dịch đáng chú ý có thể kể tới là:

- Nhóm tấn công APT-C-35 (DoNot Team) sử dụng mã độc Rafel RAT để thu thập và tải về máy chủ C&C các file tài liệu, ảnh, file nén và file cơ sở dữ liệu.

- Một số đối tượng tấn công chưa xác định đã phát tán các file PDF độc hại thông qua mạng xã hội Facebook, ứng dụng Discord nhằm phát tán mã độc RAT đánh cắp dữ liệu cookies, thông tin xác thực của người dùng trên trình duyệt Google Chrome và Edge, cùng với mã độc đào tiền ảo.

- Chiến dịch sử dụng nền tảng Trello làm nơi lưu trữ để phát tán mã độc Remcos RAT nhằm vào người dùng tại Việt Nam, Hàn Quốc cùng một số quốc gia khác.

Các đơn vị có thể tải xuống các mã IOC tại <https://alert.khonggianmang.vn/>

Danh sách một số IoC được ghi nhận:

(Máy chủ C&C Remcos RAT) 139.99.85[.]106:2404	(Remcos) 0ADE87BA165A269FD4C031772 26A148904E14BD328BDBB3179 9D2EAD59D7C2FA
--	--

(Avict Software) 3f291d07a7b0596dcd6f419e6b38645b7 7b551a2716649c12b8706d31228d79	(Avict Software) f002712b557a93da23bbf4207e5bc 57cc5e4e6e841653ffab59deb97b19 f214e
(PDF Exploit Builder) ac7598e2b4dd12ac584a288f528a94c484 570582c9877c821c47789447b780ec	(FuckCrypt) 20549f237f3552570692e6e2bb31c 4d2ddf8133c5f59f5914522e882393 70514
(FuckCrypt) 87effdf835590f85db589768b14adae2f7 6b59b2f33fae0300aef50575e6340d	(FuckCrypt) 5c42a4b474d7433bd9f1665dc914d e7b3cc7fbdb9618b0322324b53444 0737d7
(Python) 79e1cb66cb52852ca3f46a2089115e11ff f760227ae0ac13f128dda067675fbc	(Python) a4a8486c26c050ed3b3eb02c826b1 b67e505ada0bf864a223287d5b3f7a 0cde0
(PDF) d44f161b75cba92d61759ef535596912e 1ea8b6a5a2067a2832f953808ca8609	(PDF) 9c5883cf118f1d22795f7b5661573f 8099554c5a3f78d592e8917917baa 6d20f
(PDF) 2aa9459160149ecef1c9b63420eedc7fe 3a21ae0ca3e080c93fd39fef32e9c0	(PDF) 8155a6423d64f30d2994163425d3f be14a52927d3616ffacea36ddc71a6 af4b0
(PDF) c1436f65acbf7123d1a45b0898be69ba96 4f0c6d569aa350c9d8a5f187b3c0e7	(PDF) de8ecd738f1f24a94aba06f19d4263 99bc250cc5e7b848b2cbd92fc1d69 06403
(Blank-Grabber)	(Python-Stealer-Dropper)

d2bd6a05d1e30586216e73602a0536738 0ae66654cd0bccabb0414ef6810ab18	e32d2966a22243f346e06d4da5164 abab63c2700c905f22c09a18125ee4 de559
(BAT file) eb87ec49879dc44b6794bb70bd6c706e7 4694e4c2bbc1926dd4cff42e5b63cc6	(BAT file) b59ab9147214bc1682006918692fe bed4ad37e1d305c5c80dc1ee46191 4eacd2
(APT-C-35 / DoNot Team Downloader) 4ef9133773d596d1c888b0ffe36287a810 042172b0af0dfad8c2b0c9875d1c65	(APT-C-35 / DoNot Team Downloaded1) 3e9a60d5f6174bb1f1c973e9466f3e 70c74c771043ee00688e50cac5e8ef e185
(APT-C-35 / DoNot Team Uploader) 2d40e892e059850ba708f8092523efeede 759ecd6e52d8cb7752462fcd6b6f715	(APT-C-35 / DoNot Team Screen) c943fe1b8e1b17ec379d33a6e5819a 5736cb5de13564f86f1d3fba320cce baa0
(APT-C-35 / DoNot Team APK) 7f5f1586b243f477c484c34fa6243c20b3 ecf29700c6c17e23a4daf9360e2d2f	(APT-C-35 / DoNot Team APK) ecb4f5f0ee0cda289056f2f994c061 d53cfbc8ac413f2ca4da8864c68f0a 23f6
(APT-C-35 / DoNot Team APK) 4a7aeb6f510cf5d038e566a3ccd45e98a4 6463bb67eb34012c8e64444464b081	(PDF) D5483049DC32D1A57E75983993 0FE17FE31A5F513D24074710F98 EC186F06777
(PDF) 19A8201C6A3063B897D696330C1B60 BD97914514D2AE6A6C3C1796BEC2 36724A	(VBScript) 9A7F4FF5FD0A972EEDA929372 7F0EECDD7CE2CFE0A072CDF9 D3402EE9C46A48E
(VBScript)	(VBScript)

D761FE4D58FE68FC95D72871429F0F CE6055389A58F81CF0A19EB905A96 E1C38	B3AD75EEF9208D58A904030D4 4DA22C59CE7BD47ED798B0A1 4B58330A1390FE8
(VBScript) FC330BB132A345AF05FEB0D275EE EF29C7A439A04223757F33360393CF 975CA9	(VBScript) A334A9C1A658F4EBEF7BA336F 9A27693030DC444509BD9FA8F DEFE8AAAE3A133
(VBScript) E9BF261A779C1B3A023189BEF5095 79BAD8B496DCFE5E96C19CF8CC8B EA48A08	(VBScript) EE42CF45FFF12BCC9E92629554 70BFED810F3530E651FDDB0544 56264635D9D2
(VBScript) 1CBF897CCCC22A1E6D6A12766ADF 0DCEE4C103539ADD2C10C7906042E 19519F4	(DynamicWrapperX) 4EF3A6703ABC6B2B8E2CAC30 31C1E5B86FE8B377FDE9273734 9EE52BD2604379
(ShellCode) A5C9A3518F072982404E68DC6A3DC 90EDEBBF292FC1ACA6962B6CCF64 F4FE28C	0

2. Thông tin chi tiết về chiến dịch tấn công của nhóm Earth Hundun

Nhóm tấn công APT Earth Hundun nhằm vào khu vực Châu Á Thái Bình Dương sử dụng mã độc Waterbear và biến thể mới nhất Deuterebear. Mã độc Deuterebear lần đầu được ghi nhận sử dụng vào tháng 10/2022.

Mã độc Deuterebear RAT đã được cải thiện khả năng bằng cách thu gọn lại chỉ còn 20 câu lệnh, có khả năng nhận nhiều plugin hơn để cải thiện tính linh động, bổ sung các chức năng cho phép điều khiển thiết bị người dùng dễ hơn.

Các đơn vị có thể tải xuống các mã IOC tại <https://alert.khonggianmang.vn/>

Dưới đây là số IOC được ghi nhận:

*.quadrantbd[.]com	*.taishanlaw[.]com
*.bakhell[.]com	*.gelatosg[.]com
*.operatida[.]com	*.randaln[.]com
*.nestnewhome[.]com	*.dailteeau[.]com
*.lucashnancy[.]com	*.ccarden[.]com
*.availitond[.]com	*.gayionsd[.]com
*.rchitecture[.]org	*.operatida[.]com
*.centralizebd[.]com	609120ab45745bcfe8abc244ea1501e f563cb666abd9d730413c3986a76fb 23d
88336746f2cf1034871c4ee334fae0d30 c3eb101df6f3f1c94c777639293a031	3ecbca7bf2e4557e92595fe23872658 bc3337e6f77a3aff02fb7b460272de7f 4
d4b5127988fde3704193a30840e991dc 745aea051d1551c7cb6f55853c8cb9da	974c407dd918ccba245da0fb9d5a68f 123c78aacfa85cdaba2271d6ad81380 ae
3d8512a513e5f94ce49a742ae3e485377 5f05d7481b29bfacef4316d7ba3bde2	057a0e0f522cc217ba8754abbb67f8a 667c0054fe0dcda01f4930d75cd667 cc
31c76585ea703f96c95efab0778f599d8 dc5c26eea5d155ce24f614e6bfe9e8c	0

3. Tài liệu tham khảo

<https://research.checkpoint.com/2024/foxit-pdf-flawed-design-exploitation/>

https://www.trendmicro.com/en_us/research/24/e/earth-hundun-2.html